

Serial No.: 10/026,043  
Attorney Docket No.: 40116/00401  
Reference No.: 1190

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE  
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES**

**RECEIVED  
GENERAL FAX CENTER  
SEP 14 2006**

In re Application of:	)	
	)	
<b>Huayan Wang et al.</b>	)	
	)	
Serial No.: 10/026,043	)	Group Art Unit: 2132
	)	
Filed: October 25, 2001	)	Examiner: Jung W. Kim
	)	
For: SYSTEM AND METHOD FOR	)	<b>Board of Patent Appeals and</b>
UPPER LAYER ROAMING	)	<b>Interferences</b>
AUTHENTICATION	)	
	)	

Mail Stop: Appeal Brief - Patents  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

**APPEAL BRIEF UNDER 37 C.F.R. § 41.37**

In support of the Notice of Appeal filed herewith, and pursuant to 37 C.F.R. § 41.37, Appellants present this appeal brief in the above-captioned application.

This is an appeal to the Board of Patent Appeals and Interferences from the Examiner's final rejection of claims 1-21 in the Final Office Action dated June 14, 2006. The appealed claims are set forth in the attached Claims Appendix.

09/15/2006 MBINAS 00000017 10026043

02 FC:1402

500.00 OP

Serial No.: 10/026,043  
Attorney Docket No.: 40116/00401  
Reference No.: 1190

1. Real Party in Interest

This application is assigned to Symbol Technologies, Inc., the real party in interest.

RECEIVED  
CENTRAL FAX CENTER  
SEP 14 2006

2. Related Appeals and Interferences

There are no other appeals or interferences which would directly affect, be directly affected, or have a bearing on the instant appeal.

3. Status of the Claims

Claims 1-21 have been rejected in the Final Office Action. The final rejection of claims 1-21 is being appealed.

4. Status of Amendments

All amendments submitted by Appellants prior to issuance of the 6/14/06 Final Office Action have been entered. Appellants submitted an After Final Amendment on August 16, 2006. These amendments were not entered by the Examiner. (See 8/29/06 Advisory Action). Thus, appellants submit the following appeal brief regarding claims 1-21 as they were rejected by the 6/14/06 Final Office Action.

5. Summary of Claimed Subject Matter

The present invention, recited in an independent claim 1, relates to a method for authenticating a roaming device with a network. (See Specification, Fig. 2). The method generates (202), by an authentication server (10) of the network (18), authentication data associated with the roaming device (20). (See *Id.*, p. 4, l. 29 – p. 5, l. 1; p. 6, ll. 17-19; Figs. 1-2). The method sends (204), by the authentication server (10), the authentication data to access points (12, 14, 16) of the network (18). (See *Id.*, p. 5, ll. 6-8; p. 6, ll. 19-24; Figs. 1-2). The access points (12, 14, 16) are connected to the authentication server (10). (See *Id.*, p. 4, ll. 12-14; Fig. 1). When the roaming device (20) roams to a particular access point (12, 16) of the access points (12, 14, 16), the method uses (208-216) the authentication data to locally authenticate the

Serial No.: 10/026,043  
Attorney Docket No.: 40116/00401  
Reference No.: 1190

roaming device (20) at the particular access point (12, 16). (See Id., p. 7, l. 19 – p. 8, l. 20; Figs. 1-2).

The present invention, recited in an independent claim 10, relates to a method for authenticating a roaming device with a network. (See Specification, Fig. 2). The method connects (202) the roaming device (20) with an authentication server (10) upon a contact of the roaming device (20) with a first access point (14) of the network (18). (See Id., p. 4, ll. 19-22; p. 6, ll. 17-19; Figs. 1-2). The method authenticates (206) the roaming device (20) with the authentication server (10). (See Id., p. 6, ll. 18-19; Figs. 1-2). The method generates (202) authentication data for the roaming device (20). (See Id., p. 4, l. 29 – p. 5, l. 1; p. 6, ll. 17-19; Figs. 1-2). The method distributes (204), by the authentication server (10), the authentication data to the first access point (14) and a second access point (12 or 16) of the network (18). (See Id., p. 5, ll. 6-8; p. 6, ll. 19-24; Figs. 1-2). The method locally authenticates (208-216) the roaming device (20) upon a contact with the second access point (12 or 16) using the distributed authentication data. (See Id., p. 7, l. 19 – p. 8, l. 20; Figs. 1-2).

The present invention, recited in an independent claim 16, relates to a system for authenticating a roaming device with a network. (See Id., Fig. 1). The system comprises an authentication server (10) connected to the network (18). (See Id., p. 4, ll. 11-17; Fig. 1). The system also comprises first (14) and second (12 or 16) access points connected to the authentication server (10). (See Id.). The first (14) and second (12 or 16) access points are capable of communicating with the roaming device (20). (See Id., p. 4, ll. 19-24; Fig. 1). Each of the first (14) and second (12 or 16) access points include a memory arrangement capable of storing authentication data corresponding to the roaming device (20). (See Id., p. 7, ll. 3-4; Fig. 1). The authentication server (10) sends (204) the authentication data to the first (14) and second (12 or 16) access points upon an initial authentication procedure of the roaming device (20) with the first access point (14). (See Id., p. 5, ll. 6-8; p. 6, ll. 19-24; Figs. 1-2). The second access point (12 or 16) locally authenticates (208-216) the roaming device (20) upon a contact of the roaming device (20) with the second access point (12 or 16). (See Id., p. 7, l. 19 – p. 8, l. 20; Figs. 1-2).

The present invention, recited in an independent claim 19, relates to a method for authenticating a roaming device with a network. (See Id., Fig. 2). With an authentication server (10), the method receives (202) an authentication request (802.11 Probe/Probe Response) from

Serial No.: 10/026,043  
Attorney Docket No.: 40116/00401  
Reference No.: 1190

the roaming device (20). (See Id., p. 4, ll. 19-22; p. 6, ll. 17-19; Figs. 1-3). The request is encrypted with a first shared code. (See Id., p. 10, ll. 1-3). With the authentication server (10), the method generates (202) a session key (EAP Identity) associated with the roaming device (20). (See Id., p. 4, l. 29 – p. 5, l. 1; p. 6, ll. 17-19; Figs. 1-2). The method sends (204) the session key (EAP Identity) to an access point (12, 14, 16) of the network (18). (See Id., p. 5, ll. 6-8; p. 6, ll. 19-24; Figs. 1-2). The session key (EAP Identity) is encrypted with a second shared code. (See Id., p. 10, ll. 7-9). The method utilizes (208-216) the session key (EAP Identity) to authenticate the roaming device (20) at the access point (12, 14, 16) and to encrypt data exchanged between the roaming device (20) and the access point (12, 14, 16). (See Id., p. 7, l. 19 – p. 8, l. 20; p. 10, ll. 9-12; Figs. 1-2).

6. Grounds of Rejection to be Reviewed on Appeal

I. Whether claims 1-3, 6, 10-12, 14, and 16-18 are unpatentable under 35 U.S.C. § 103(a) over U.S. Pat. No. 6,851,050 to Singhal et al. (Singhal) in view of U.S. Pat. No. 6,760,444 to Leung (Leung).

II. Whether claims 4-5 are unpatentable under 35 U.S.C. § 103(a) over U.S. Pat. No. 6,851,050 to Singhal et al. (Singhal) in view of U.S. Pat. No. 6,760,444 to Leung (Leung) in further view of U.S. Pat. No. 5,408,683 to Ablay et al. (Ablay).

III. Whether claims 7-8 and 13 are unpatentable under 35 U.S.C. § 103(a) over U.S. Pat. No. 6,851,050 to Singhal et al. (Singhal) in view of U.S. Pat. No. 6,760,444 to Leung (Leung) in further view of U.S. Pat. No. 6,452,910 to Vij et al. (Vij).

IV. Whether claim 9 is unpatentable under 35 U.S.C. § 103(a) over U.S. Pat. No. 6,851,050 to Singhal et al. (Singhal).

V. Whether claims 15 and 19-20 are unpatentable under 35 U.S.C. § 103(a) over U.S. Pat. No. 6,851,050 to Singhal et al. (Singhal) in view of U.S. Pat. No. 6,760,444 to Leung (Leung) in further view of U.S. Pat. Pub. No. 2002/0174335 to Zhang et al. (Zhang).

Serial No.: 10/026,043  
Attorney Docket No.: 40116/00401  
Reference No.: 1190

VI. Whether claim 21 is unpatentable under 35 U.S.C. § 103(a) over U.S. Pat. No. 6,851,050 to Singhal et al. (Singhal) in view of U.S. Pat. No. 6,760,444 to Leung (Leung) in further view of U.S. Pat. Pub. No. 2002/0174335 to Zhang et al. (Zhang) in further view of U.S. Pat. No. 6,178,506 to Quick, Jr. (Quick).

7. Argument

I. The Rejection of Claims 1-3, 6, 10-12, 14, and 16-18 Under 35 U.S.C. § 103(a) Over U.S. Pat. No. 6,851,050 to Singhal et al. In View of U.S. Pat. No. 6,760,444 to Leung Should Be Reversed.

A. The Examiner's Rejection

In the Final Office Action, the Examiner rejected claims 1-3, 6, 10-12, 14, and 16-18 under 35 U.S.C. § 103(a) as being unpatentable over Singhal in view of Leung. (See 6/14/06 Office Action, p. 4, ll. 2-4).

Singhal is directed toward providing location-independent packet routing and secure access in a wireless networking environment thereby enabling client devices to travel within the environment. An address translation process that is transparent to the client and server is automatically performed as the device roams through the environment. The secure access techniques provide user-centric authentication and allow policy-driven packet filtering. (See Singhal, Abstract). When the client first communicates with the access point, assuming no session key already exists between the client and the access point, the access point communicates with an authentication server to obtain security information for the client. (See Id., col. 18, ll. 39-47). Once the client has been authenticated, the authentication data is sent to a routing coordinator, which stores the data in a lookup table. (See Id., col. 18, ll. 61-64).

Leung is directed toward authenticating a mobile node. A server is configured to provide a plurality of security associations associated with a plurality of mobile nodes. A packet identifying a mobile node is sent to the server from a Home Agent. A security association for the mobile node identified in the packet may then be obtained from the server. The security association is sent to the network device to permit authentication. (See Leung, Abstract). Each Home Agent is associated with a set number of mobile nodes. (See Id., col. 6, ll. 56-59). Each mobile node requires authentication by contacting that mobile node's Home Agent. (See Id.)

Serial No.: 10/026,043  
Attorney Docket No.: 40116/00401  
Reference No.: 1190

**B. The Cited Patents Describe No Motivation To Combine Such Technologies And Would Not Have Been Obvious To One Skilled In The Art, Thereby Improperly Combined.**

The Examiner correctly stated that Singhal does not disclose "using the authentication data to locally authenticate the roaming device at the particular access point," as recited in claim 1. (See 6/14/06 Office Action, p. 4, ll. 15-16). The Examiner attempted to cure this deficiency with Leung. However, it is respectfully submitted that the Examiner improperly combined the teachings of Singhal with the teachings of Leung. Specifically, the teachings of Leung teach away from the teachings of Singhal.

As discussed above, Singhal teaches that upon the client first communicating with an access point, a client authentication module (*i.e.*, mobile device) communicates with a server authentication module (*i.e.*, access point) to provide the user's authentication credentials. (See Singhal, col. 18, ll. 39-45). The server authentication module connects with an authentication server where a key is provided for authentication purposes. (See *Id.*, col. 18, ll. 49-50). Subsequently, the key is provided to a routing coordinator that stores it in a lookup table. (See *Id.*, col. 18, ll. 61-64). Each subsequent access point contacts the routing coordinator to access the lookup table for authentication of the client authentication module. (See *Id.*, col. 18, l. 65 – col. 19, l. 3). That is, the routing coordinator sends "authentication data" from the routing coordinator to the access point each time the mobile device enters the coverage area of that access point (*i.e.*, individual remote authentications take place).

Also, as discussed above, Leung teaches that a single Home Agent is responsible for a set of mobile nodes. (See Leung, col. 6, ll. 47-49). A mobile node is authenticated by sending security association data to the mobile node's Home Agent. (See *Id.*, col. 6, ll. 56-59). Because no other Home Agent contains the security data relevant to a given mobile node, the mobile node's Home Agent is contacted. The use of a Home Agent effectively reduces the amount of traffic that would normally occur since the authentication server becomes unnecessary after the Home Agent receives the authentication data.

Therefore, Leung is teaching away from Singhal because one specific objective of Leung is to prevent repetitive accesses to the authentication server. In contrast, Singhal teaches that each access point must contact the routing coordinator every time a mobile node enters an access point. That is, one either desires a system as taught by Singhal where there are multiple

Serial No.: 10/026,043  
Attorney Docket No.: 40116/00401  
Reference No.: 1190

communications by multiple access points with the authentication server or a system as taught by Leung having a single communication between a Home Agent and the authentication server. Any cure for the multiple communications of Singhal results in Leung by itself, not a hybrid of Singhal (multiple communications) and Leung (single communication). The two references are incompatible.

It appears to the appellants that the Examiner uses Leung for a narrow exemplary embodiment where a mobile node initially registers with a foreign agent and roams into the mobile node's Home Agent. Appellants respectfully submit that this furthers the improper combination argument discussed above. That is, the Examiner cannot merely select portions of prior art. There must be some motivation to combine the teachings of the prior art. The fact that Singhal discloses an authentication procedure and Leung discloses a method of authenticating should not preclude the present invention since, as discussed above, such a combination was improper and would, therefore, not have been obvious to one skilled in the art.

In rejecting claims under 35 U.S.C. §103, the Examiner bears the initial burden of establishing a prima facie case of obviousness. In re Oetiker, 977 F. 2d 1443, 1445, 24 USPQ2d 1442, 1444 (Fed. Cir. 1992). See also In re Piasecki, 745 F. 2d 1468, 1472, 223 USPQ 785, 788 (Fed. Cir. 1984). The Examiner can satisfy this burden by showing that some objective teaching in the prior art of knowledge generally available to one of ordinary skill in the art suggest the claimed subject matter. In re Fine, 837 F. 2d 1071, 1074, 5 USPQ2d 1596, 1598 (Fed. Cir. 1988).

When determining obviousness, "[t]he factual inquiry whether to combine references must be through and searching." In re Lee, 277 F. 3d 1338, 1343, 61 USPQ 1430, 1433 (Fed. Cir. 2002), citing McGinley v. Franklin Sports, Inc., 262 F. 3d 1339, 1351-52, 60 USPQ2d 1001, 1008 (Fed. Cir. 2001). "It must be based on objective evidence of record." Id. "Broad conclusory statements regarding the teaching of multiple references, standing alone, are not 'evidence.'" In re Dembiczak, 175 F. 3d 994, 999, 50 USPQ2d 1614, 1617. "Mere denials and conclusory statements, however, are not sufficient to establish a genuine issue of material fact." Dembiczak, 175 F. 3d at 1000, 50 USPQ2d at 1617, citing McElmurry v. Ark. Power & Light Co., 995 F. 2d 1576, 1578, 27 USPQ2d 1129, 1131 (Fed. Cir. 1993).

The suggestion in the Office Action that the combination of prior art references "would be obvious to one having ordinary skill in the art..." is respectfully refuted. One may not

Serial No.: 10/026,043  
Attorney Docket No.: 40116/00401  
Reference No.: 1190

utilize the teaching of the present application as a road map to pick and choose amongst prior art references for the purposes of attempting to arrive at the presently disclosed invention. The Federal Circuit has identified three possible sources for motivation to combine references including the nature of the problem to be solved, the teaching of the prior art, and the knowledge of persons of ordinary skill in the art. (See, In re Rouffet, U. S. Court of Appeals Federal Circuit, U.S.P.Q. 2d 1453, 1458). There must be a specific principle that would motivate a skilled artisan, with no knowledge of the present invention, to combine the prior art as suggested in the Office Action. The use of hindsight in the selection of references is forbidden in comprising the case of obviousness. Lacking a motivation to combine references, a proper case of obviousness is not shown (see, In re Rouffet, 1458).

The U.S. Court of Appeals for the Federal Circuit (the "Federal Circuit") restated the legal test applicable to rejections under 35 U.S.C. §103 (a) in the In re Rouffet holding. The Court stated:

[V]irtually all [inventors] are combinations of old elements. Therefore an Examiner may often find every element of a claimed invention in the prior art. Furthermore, rejecting parents solely by finding prior art corollaries for the claimed elements would permit an Examiner to use the claimed invention itself as a blueprint for piecing together elements in the prior art to defeat the patentability of the claimed invention. Such an approach would be "an illogical and inappropriate process by which to determine patentability." To prevent the use of hindsight based on the invention to defeat patentability of the invention. This court requires the Examiner to show a motivation to combine the references that create the case of obviousness. The Board (of Appeals) did not, however, explain what specific understanding of technological principle within the knowledge of one of ordinary skill in the art would have suggested the combination. ... To counter this potential weakness in the obviousness contract the suggestion to combine requirements stands as a critical safeguard against hindsight analysis and rote application of the legal test for obviousness.

In re Rouffet, 47 USPQ2d 1457-58 (Fed. Cir., July 15, 1998) (citations omitted, emphasis added).

More recently, the Federal Circuit again dealt with what is required to show a motivation to combine references under 35 U. S. C. §103 (a). In this case the Court reversed the decision of the Board of appeals stating:

[R]ather than pointing to specific information in Holiday or Shapiro that suggest the combination..., the Board instead described in details the similarities between



Serial No.: 10/026,043  
Attorney Docket No.: 40116/00401  
Reference No.: 1190

the Holiday and Shapiro references and the claimed invention, noting that one reference or the other in combination with each other... described all of the limitations of the pending claims. Nowhere does the Board particularly identify any suggestion, teaching, or motivation to combine the ... references, not does the Board make specific—or even inferential—findings concerning the identification of the relevant art, the level of ordinary skill in the art, the nature of the problem to be solved, or any factual findings that might serve to support a proper analysis.

In re Dembiczak, 50USPQ2d 1614, 1618 (Fed. Cir., April 28, 1999) (citations omitted).

Thus, from both In re Rouffet and In re Dembiczak it is clear that the Federal Circuit requires a specific identification of a suggestion, motivation, or teaching why one of ordinary skill in the art would have been motivated to select the references and combine them.

The Examiner's reasoning for the motivation, namely, that those skilled in the art would have been motivated to combine Singhal with Leung, could only have been made with hindsight based on the teaching of the present disclosure. The Examiner's reasoning for the motivation for combining the references is nowhere recognized in the prior art nor does the Examiner attempt to make any showing that the art recognized such problems. In fact, as described above, the two systems operate in two different, wholly incompatible manners.

Where a feature is not shown or suggested in the prior art references themselves, the Federal Circuit has held that the skill in the art will rarely suffice to show the missing feature. Al-Site Corp. v. VSI International Inc., 174 F. 3d 1308, 50 USPQ2d 1161 (Fed. Cir. 1999) (Rarely, however, will the skill in the art component operate to supply missing knowledge or prior art to reach an obviousness judgment).

Thus, Appellants again respectfully submit that the Examiner has used impermissible hindsight to reject claims 1-3, 6, 10-12, 14, and 16-18 under 35 U.S.C. §103 (a). As discussed above, the Federal Circuit in In re Rouffet stated that virtually all inventions are combinations of old elements. Therefore an Examiner may often find every element of a claimed invention in the prior art. To prevent the use of hindsight based on the invention to defeat patentability of the invention, the Examiner is required to show a motivation to combine the references that create the case of obviousness. Appellants respectfully submit that the Examiner has not met this burden.

Serial No.: 10/026,043  
Attorney Docket No.: 40116/00401  
Reference No.: 1190

The mere fact that the prior art device could be modified so as to produce the claimed device is not a basis for an obviousness rejection unless the prior art suggested the desirability of the modification. See, In re Gordon, 733 F.2d 900, 902 (Fed. Cir. 1984), and In re Laskowski, 871 F.2d 115, 117 (Fed. Cir. 1989).

The only suggestion that can be found anywhere for making these combinations appears to come from the present patent application itself.

In consideration of the use of improper hindsight for rendering a claim obvious in light of prior art, the Federal Circuit has stated that "to draw on hindsight knowledge of the patented invention, when the prior art does not contain or suggest that knowledge is to use the invention as a template for its own reconstruction – an illogical and inappropriate process by which to determine patentability." (Sensonic, Inc. v. Aerosonic Corp., 81F.3d 1566, 38 USPQ2d 1551 (Fed. Cir. 1996). "To imbue one of ordinary skill in the art with knowledge of the invention ensued, when no prior art reference or references of record convey or suggest that knowledge, is to fall victim to the insidious effect of a hindsight syndrome wherein that which only the inventor taught is used against each teacher." (In re Zurko, 111 F.3d 887, 42 USPQ2d 1476 (Fed. Cir. 1997). A critical step is analyzing the patentability of claims pursuant to section 103 (a) is casting the mind back to the time of invention, to consider the thinking of one of ordinary skill in the art, guided only by the prior art references and the then-accepted wisdom in the field (cited reference omitted). Close adherence to this methodology is especially important in cases where the very ease with which the invention can be understood may prompt one ' to fall victim to the insidious effect of a hindsight syndrome wherein that which only the invention taught is used against its teacher (cited reference omitted).'" (In re Kotzab, 208 F.3d 1352, 54 USPQ2d 1308 (Fed. Cir. 1997).

Appellants respectfully maintain that there is no suggestion in the prior art references to make the combinations in the manner proposed by the Examiner to achieve the Appellants' claimed invention.

Considering MPEP 2143, it is stated:

"THE PRIOR ART MUST SUGGEST THE DESIRABILITY OF THE CLAIMED INVENTION ... The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, not in applicant's disclosure. In re Vaeck, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991)." And, "FACT THAT

Serial No.: 10/026,043  
Attorney Docket No.: 40116/00401  
Reference No.: 1190

REFERENCES CAN BE COMBINED OR MODIFIED IS NOT SUFFICIENT TO ESTABLISH PRIMA FACIE OBVIOUSNESS... The mere fact that references can be combined or modified does not render the resultant combination obvious unless the prior art also suggests the desirability of the combination. *In re Mills*, 916 F. 2d 680, 16 USPQ2d 1430 (Fed. Cir. 1990)... Although a prior art device "may be capable of being modified to run the way the apparatus is claimed, there must be a suggestion or motivation in the reference to do so." 916 F.2d at 682, 16 USPQ2d at 1432.)" There is no such suggestion in either Singhal or Leung that would justify such a combination.

It is respectfully submitted that in light of the state of the law as set forth by the Federal Circuit and the Examiner's lack of specificity with regard to the motivation to combine the cited references, that none of the suggested combinations of prior art utilized to reject each of claims 1-3, 6, 10-12, 14, and 16-18 finds proper motivation for combination. Further, since the Examiner's rejections acknowledge that the prior art alone does not show the claimed features, it is respectfully submitted that claims 1-3, 6, 10-12, 14, and 16-18 are not obvious in light of the cited references.

Thus, it is respectfully submitted that the Examiner improperly combined the teachings of Singhal with the teachings of Leung. Accordingly, it is respectfully submitted that claims 1-3, 6, 10-12, 14, and 16-18 are therefore allowable.

II. The Rejection of Claims 4-5 Under 35 U.S.C. § 103(a) Over U.S. Pat. No. 6,851,050 to Singhal et al. In View of U.S. Pat. No. 6,760,444 to Leung In Further View of U.S. Pat. No. 5,408,683 to Ablay et al. Should Be Reversed.

A. The Examiner's Rejection

In the Final Office Action, the Examiner rejected claims 4-5 under 35 U.S.C. § 103(a) as being unpatentable over Singhal in view of Leung in further view of Ablay. (See 6/14/06 Office Action, p. 9, ll. 15-17). Singhal and Leung were discussed above.

Ablay is directed toward tracking subscribers in a networked radio communications system. The subscribers are able to roam among a plurality of coverage areas which are serviced by a plurality of transmitters. The transmitters are coupled to a central processor which access a memory device for storing subscriber records and site records. The method relies on the subscriber sending an inbound message which includes its current location.

Serial No.: 10/026,043  
Attorney Docket No.: 40116/00401  
Reference No.: 1190

(See Ablay, abstract). Ablay does not include any disclosure concerning a local authentication for the subscribers at the plurality of transmitters.

B. The Cited Patents Describe No Motivation To Combine Such Technologies And Would Not Have Been Obvious To One Skilled In The Art. Thereby Improperly Combined.

As discussed above, Singhal was improperly combined with Leung. The further combination of Ablay maintains the improper combination. Thus, it is respectfully submitted that claims 4-5 which depend from and, therefore, include all of the limitations of an allowable claim are also allowable.

III. The Rejection of Claims 7-8 and 13 Under 35 U.S.C. § 103(a) Over U.S. Pat. No. 6,851,050 to Singhal et al. In View of U.S. Pat. No. 6,760,444 to Leung In Further View of U.S. Pat. No. 6,452,910 to Vij et al. Should Be Reversed.

A. The Examiner's Rejection

In the Final Office Action, the Examiner rejected claims 7-8 and 13 under 35 U.S.C. § 103(a) as being unpatentable over Singhal in view of Leung in further view of Vij. (See 6/14/06 Office Action, p. 11, ll. 3-5). Singhal and Leung were discussed above.

Vij is directed toward a wireless bridge that connects two previously incompatible technologies within a single device to leverage the strengths of each. The wireless bridge marries a personal area network technology with a wireless local area network to provide a wireless system for peripheral devices. (See Vij, abstract). Vij concerns the separation and shielding required of potentially conflicting technologies to inter-operate. That is, there is no disclosure in Vij concerning a local authentication for a roaming device at a particular access point.

B. The Cited Patents Describe No Motivation To Combine Such Technologies And Would Not Have Been Obvious To One Skilled In The Art. Thereby Improperly Combined.

As discussed above, Singhal was improperly combined with Leung. The further combination of Vij maintains the improper combination. Thus, it is respectfully submitted that

Serial No.: 10/026,043  
Attorney Docket No.: 40116/00401  
Reference No.: 1190

claims 7-8 and 13 which depend from and, therefore, include all of the limitations of allowable claims are also allowable.

IV. The Rejection of Claim 9 Under 35 U.S.C. § 103(a) Over U.S. Pat. No. 6,851,050 to Singhal et al. With The Rejection Of Claim 1 Under 35 U.S.C. § 103(a) As Being Unpatentable Over U.S. Pat. No. 6,851,050 to Singhal et al. In View of U.S. Pat. No. 6,760,444 to Leung Incorporated By Reference Should Be Reversed.

A. The Examiner's Rejection

In the Final Office Action, the Examiner rejected claim 9 under 35 U.S.C. § 103(a) as being unpatentable over Singhal with the rejection of claim 1 under 35 U.S.C. § 103(a) as being unpatentable in view of Singhal in view of Leung incorporated by reference. (See 6/14/06 Office Action, p. 13, ll. 8-9). Singhal and Leung were discussed above.

B. The Cited Patents Describe No Motivation To Combine Such Technologies And Would Not Have Been Obvious To One Skilled In The Art. Thereby Improperly Combined.

As discussed above, Singhal was improperly combined with Leung. Thus, it is respectfully submitted that claim 9 which depends from and, therefore, includes all of the limitations of an allowable claim is also allowable.

V. The Rejection of Claims 15 and 19-20 Under 35 U.S.C. § 103(a) Over U.S. Pat. No. 6,851,050 to Singhal et al. In View of U.S. Pat. No. 6,760,444 to Leung In Further View of U.S. Pat. Pub. No. 2002/0174335 to Zhang et al. Should Be Reversed.

A. The Examiner's Rejection

In the Final Office Action, the Examiner rejected claims 15 and 19-20 under 35 U.S.C. § 103(a) as being unpatentable over Singhal in view of Leung in further view of Zhang. (See 6/14/06 Office Action, p. 14, ll. 6-9). Singhal and Leung were discussed above.

Zhang is directed toward converging both the authentication, accounting, and authorization process with data transmissions at the Internet Protocol layer. (See Zhang, abstract). Zhang still maintains a communication with the access point to an authentication

Serial No.: 10/026,043  
Attorney Docket No.: 40116/00401  
Reference No.: 1190

server to authenticate mobile devices. That is, there is no disclosure in Zhang concerning a local authentication for a roaming device at a particular access point.

B. The Cited Patents Describe No Motivation To Combine Such Technologies And Would Not Have Been Obvious To One Skilled In The Art, Thereby Improperly Combined.

As discussed above, Singhal was improperly combined with Leung. The further combination of Zhang maintains the improper combination. Thus, it is respectfully submitted that claim 15 which depends from and, therefore, includes all of the limitations of an allowable claim is also allowable. It is also respectfully submitted that claims 19-20 are also allowable as the basis of the Examiner's rejection for these claims involves the improper combination of Singhal with Leung.

VI. The Rejection of Claim 21 Under 35 U.S.C. § 103(a) Over U.S. Pat. No. 6,851,050 to Singhal et al. In View of U.S. Pat. No. 6,760,444 to Leung In Further View of U.S. Pat. Pub. No. 2002/0174335 to Zhang et al. In Further View of U.S. Pat. No. 6,178,506 to Quick, Jr. Should Be Reversed.

A. The Examiner's Rejection

In the Final Office Action, the Examiner rejected claim 21 under 35 U.S.C. § 103(a) as being unpatentable over Singhal in view of Leung in further view of Zhang in further view of Quick. (See 6/14/06 Office Action, p. 16, ll. 7-9). Singhal, Leung, and Zhang were discussed above.

Quick is directed toward a pin identification number to transfer a subscription for wireless service to a new wireless terminal. (See Quick, abstract). Quick concerns a subscription at the mobile device level and incorporates conventional authentication procedures where the access point communicates with an authentication server to authenticate the mobile device. That is, there is no disclosure in Quick concerning a local authentication for a roaming device at a particular access point.

B. The Cited Patents Describe No Motivation To Combine Such Technologies And Would Not Have Been Obvious To One Skilled In The Art, Thereby Improperly Combined.

Serial No.: 10/026,043  
Attorney Docket No.: 40116/00401  
Reference No.: 1190

As discussed above, Singhal was improperly combined with Leung. The further combination of Zhang and Quick maintains the improper combination. Thus, it is respectfully submitted that claim 21 which depends from and, therefore, includes all of the limitations of an allowable claim is also allowable.

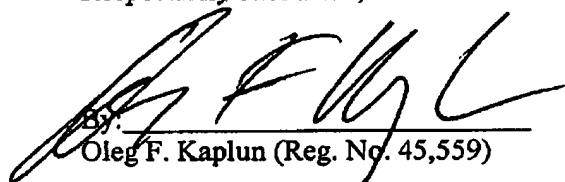
Serial No.: 10/026,043  
Attorney Docket No.: 40116/00401  
Reference No.: 1190

8. Conclusion

For the reasons set forth above, Appellants respectfully request that the Board reverse the rejection of the claims by the Examiner under 35 U.S.C. § 103(a), and indicate that claims 1-21 are allowable.

Respectfully submitted,

Date: September 14, 2006

  
By: \_\_\_\_\_  
Oleg F. Kaplun (Reg. No. 45,559)

Fay Kaplun & Marcin, LLP  
150 Broadway, Suite 702  
New York, NY 10038  
Tel: (212) 619-6000  
Fax: (212) 619-0276



Serial No.: 10/026,043  
Attorney Docket No.: 40116/00401  
Reference No.: 1190

RECEIVED  
CENTRAL FAX CENTER  
SEP 14 2006

**CLAIMS APPENDIX**

1. (Rejected) A method for authenticating a roaming device with a network, comprising the steps of:

generating, by an authentication server of the network, authentication data associated with the roaming device;

sending, by the authentication server, the authentication data to access points of the network, the access points being connected to the authentication server; and

when the roaming device roams to a particular access point of the access points, using the authentication data to locally authenticate the roaming device at the particular access point.

2. (Rejected) The method according to claim 1, further comprising the step of:  
storing the authentication data in a memory arrangement of each of the access points.

3. (Rejected) The method according to claim 1, wherein the sending step includes the substeps of:  
encrypting the authentication data; and  
sending the encrypted authentication data to selected access points of the access points.

4. (Rejected) The method according to claim 3, wherein the sending step includes the substeps of:  
determining at least one access point of the access points using prediction algorithms to anticipate where the roaming device will roam; and  
sending the encrypted authentication data to the at least one access point.

5. (Rejected) The method according to claim 3, wherein the sending step includes the substep of sending the encrypted authentication data to all the access points.

6. (Rejected) The method according to claim 1, further comprising the preliminary steps of:  
determining if the particular access point has authentication data associated with the roaming device;

Serial No.: 10/026,043  
Attorney Docket No.: 40116/00401  
Reference No.: 1190

if the determination is positive, proceed to the step of using the authentication data to locally authenticate the roaming device at the particular access point; and

if the determination is negative, proceed to the step of generating, by an authentication server of the network, authentication data associated with the roaming device.

7. (Rejected) The method according to claim 6, wherein the step of using the authentication data to locally authenticate the roaming device further comprises reassociating the roaming device with the particular access point of the access points by exchanging identification information.

8. (Rejected) The method according to claim 7, wherein the reassociating step further includes the substeps of:

searching a memory arrangement of the particular access point for the authentication data associated with the roaming device; and

if the authentication data is found, performing a mutual authentication procedure between the roaming device and the particular access point.

9. (Rejected) The method according to claim 1, wherein the generating step further includes the steps of:

receiving an encrypted authentication request from the roaming device;  
determining that the roaming device can be granted access to network services; and  
generating an encrypted session key associated with the roaming device in the authentication server.

10. (Rejected) A method for authenticating a roaming device with a network, comprising the steps of:

connecting the roaming device with an authentication server upon a contact of the roaming device with a first access point of the network;  
authenticating the roaming device with the authentication server;  
generating authentication data for the roaming device;

Serial No.: 10/026,043  
Attorney Docket No.: 40116/00401  
Reference No.: 1190

distributing, by the authentication server, the authentication data to the first access point and a second access point of the network; and

locally authenticating the roaming device upon a contact with the second access point using the distributed authentication data.

11. (Rejected) The method according to claim 10, further comprising the step of:  
authenticating the roaming device with the authentication server if the local authentication of the roaming device fails.

12. (Rejected) The method according to claim 10, wherein the distributing step further includes the substep of:  
distributing an encrypted session key to the first and second access points.

13. (Rejected) The method according to claim 10, wherein the locally authenticating step further includes the substeps of:  
exchanging identification data between the roaming device and the second access point;  
and  
correlating the identification data with the distributed authentication data.

14. (Rejected) The method according to claim 10, further comprising the step of:  
establishing a shared secret encryption between the authentication server and the first and second access points.

15. (Rejected) The method according to claim 10, wherein the authentication server is a remote authentication dial-in user server.

16. (Rejected) A system for authenticating a roaming device with a network, comprising:  
an authentication server connected to the network; and  
first and second access points connected to the authentication server, the first and second access points being capable of communicating with the roaming device, each of the first and

Serial No.: 10/026,043  
Attorney Docket No.: 40116/00401  
Reference No.: 1190

second access points including a memory arrangement capable of storing authentication data corresponding to the roaming device,

wherein the authentication server sends the authentication data to the first and second access points upon an initial authentication procedure of the roaming device with the first access point, and

wherein the second access point locally authenticates the roaming device upon a contact of the roaming device with the second access point.

17. (Rejected) The system according to claim 16, wherein the second access point authenticates the roaming device with the authentication server if the authentication data is not found in the memory arrangement of the second access point.

18. (Rejected) The system according to claim 16, wherein the second access point authenticates the roaming device with the authentication server if the local authentication of the roaming device at the second access point fails.

19. (Rejected) A method for authenticating a roaming device with a network, comprising the steps of:

with an authentication server, receiving an authentication request from a roaming device, the request being encrypted with a first shared code;

with the authentication server, generating a session key associated with the roaming device;

sending the session key to an access point of the network, the session key being encrypted with a second shared code; and

utilizing the session key to authenticate the roaming device at the access point, and to encrypt data exchanged between the roaming device and the access point.

20. (Rejected) The method according to claim 19, further comprising the step of:

sending the encrypted session key to a further access point of the network to authenticate the roaming device at the further access point.

Serial No.: 10/026,043  
Attorney Docket No.: 40116/00401  
Reference No.: 1190

21. (Rejected) The method according to claim 19, further comprising the steps of:  
generating a first key of the session key to perform authentication of the roaming device  
at the access point; and  
generating a second key of the session key to encrypt data exchanges between the  
roaming device and the access point, the second key being different from the first key.

Serial No.: 10/026,043  
Attorney Docket No.: 40116/00401  
Reference No.: 1190

**EVIDENCE APPENDIX**

No evidence has been entered or relied upon in the present appeal.

RECEIVED  
CENTRAL FAX CENTER  
SEP 14 2006

Serial No.: 10/026,043  
Attorney Docket No.: 40116/00401  
Reference No.: 1190

**RELATED PROCEEDING APPENDIX**

No decisions have been rendered regarding the present appeal or any proceedings related thereto.

RECEIVED  
CENTRAL FAX CENTER  
SEP 14 2006